What is claimed is:

1.   A system for intrusion detection data collection using a protocol
2   stack multiplexor, comprising:
3   a hierarchical protocol stack defined within kernel memory space and
4   comprising a plurality of communicatively interfaced protocol layers, each such
5   protocol layer comprising one or more procedures for processing data packets;
6   a data frame processed through the protocol stack, the data frame
7   comprising a plurality of recursively encapsulated data packets which are each
8   encoded with a protocol recognized by one of the protocol layers; and
9   a protocol stack multiplexor collecting data directly from the protocol
10   stack from at least one of the processed data packets, comprising:
11   an interface interfacing directly into at least one such protocol
12   layer through redirected references to the data packet processing procedures
13   comprised within the at least one such protocol layer; and
14   a logical reference to the processed data packets obtained from the
15   interfaced protocol layer, the logical reference referring to a memory block in the
16   kernel memory space within which the processed data packets are stored and
17   provided to an intrusion detection analyzer executing within user memory space.

1   2.   A system according to Claim 1, further comprising:
2   a network hardware interface in a link protocol layer logically located at a
3   device end of the protocol stack;
4   an application software interface in a transport protocol layer logically
5   located at a user end of the protocol stack; and
6   the protocol stack multiplexor tapping the collected data from the protocol
7   stack between and through the link protocol layer and the transport protocol layer.

1   3.   A system according to Claim 2, wherein the protocol stack
2   comprises a Transmission Control Protocol/Internet Protocol-compliant (TCP/IP)
3   protocol stack.

1   4.   A system according to Claim 1, further comprising:

2   a read queue associated with each protocol layer storing incoming data

3 frames;

4   a write queue associated with each protocol layer storing outgoing data

5 frame; and

6   the protocol stack multiplexor retrieving the logical reference to the

7 processed data packets from at least one of the read queue and the write queue.

1   5.   A system according to Claim 1, further comprising:

2   a module switch table in the kernel memory space storing the references to

3 the data packet processing procedures comprised within the at least one such

4 protocol layer; and

5   an initialization module in the protocol stack multiplexor replacing select

6 procedure references in the module switch table with references to data collection

7 procedures in the protocol stack multiplexor.

1   6.   A system according to Claim 5, wherein one such protocol layer

2 comprises a Transmission Control Protocol-compliant (TCP) protocol layer,

3 further comprising:

4   the initialization module augmenting the procedure references in the

5 module switch table for the procedures for processing data frames for the TCP

6 protocol layer with references to TCP data collection procedures in the protocol

7 stack multiplexor.

1   7.   A system according to Claim 5, wherein one such protocol layer

2 comprises a User Datagram Protocol-compliant (UDP) protocol layer, further

3 comprising:

4   the initialization module replacing the procedure references in the module

5 switch table for the procedures for processing incoming data frames for the UDP

6 protocol layer with references to UDP data collection procedures in the protocol

7 stack multiplexor.

1   8.   A method for intrusion detection data collection using a protocol

2   stack multiplexor, comprising:

3   defining a hierarchical protocol stack within kernel memory space and

4   comprising a plurality of communicatively interfaced protocol layers, each such

5   protocol layer comprising one or more procedures for processing data packets;

6   processing a data frame through the protocol stack, the data frame

7   comprising a plurality of recursively encapsulated data packets which are each

8   encoded with a protocol recognized by one of the protocol layers; and

9   collecting data directly from the protocol stack from at least one of the

10   processed data packets using a protocol stack multiplexor, comprising:

11   interfacing directly into at least one such protocol layer through

12   redirected references to the data packet processing procedures comprised within

13   the at least one such protocol layer;

14   obtaining a logical reference to the processed data packets from the

15   interfaced protocol layer, the logical reference referring to a memory block in the

16   kernel memory space within which the processed data packets are stored; and

17   providing the logical reference to an intrusion detection analyzer

18   executing within user memory space.

1   9.   A method according to Claim 8, further comprising:

2   providing a network hardware interface in a link protocol layer logically

3   located at a device end of the protocol stack;

4   providing an application software interface in a transport protocol layer

5   logically located at a user end of the protocol stack; and

6   tapping the collected data from the protocol stack between and through the

7   link protocol layer and the transport protocol layer.

1   10.   A method according to Claim 9, wherein the protocol stack

2   comprises a Transmission Control Protocol/Internet Protocol-compliant (TCP/IP)

3   protocol stack.

1   11.   A method according to Claim 8, further comprising:

2   storing incoming data frames in a read queue associated with each

3 protocol layer;

4   storing outgoing data frame in a write queue associated with each protocol

5 layer; and

6   retrieving the logical reference to the processed data packets from at least

7 one of the read queue and the write queue.

1   12.   A method according to Claim 8, further comprising:

2   storing the references to the data packet processing procedures comprised

3 within the at least one such protocol layer in a module switch table in the kernel

4 memory space; and

5   replacing select procedure references in the module switch table with

6 references to data collection procedures in the protocol stack multiplexor.

1   13.   A method according to Claim 12, wherein one such protocol layer

2 comprises a Transmission Control Protocol-compliant (TCP) protocol layer,

3 further comprising:

4   augmenting the procedure references in the module switch table for the

5 procedures for processing data frames for the TCP protocol layer with references

6 to TCP data collection procedures in the protocol stack multiplexor.

1   14.   A method according to Claim 12, wherein one such protocol layer

2 comprises a User Datagram Protocol-compliant (UDP) protocol layer, further

3 comprising:

4   replacing the procedure references in the module switch table for the

5 procedures for processing incoming data frames for the UDP protocol layer with

6 references to UDP data collection procedures in the protocol stack multiplexor.

1   15.   A storage medium for intrusion detection data collection using a

2 protocol stack multiplexor, comprising:

3   defining a hierarchical protocol stack within kernel memory space and

4   comprising a plurality of communicatively interfaced protocol layers, each such

5   protocol layer comprising one or more procedures for processing data packets;

6   processing a data frame through the protocol stack, the data frame

7   comprising a plurality of recursively encapsulated data packets which are each

8   encoded with a protocol recognized by one of the protocol layers; and

9   collecting data directly from the protocol stack from at least one of the

10   processed data packets using a protocol stack multiplexor, comprising:

11   interfacing directly into at least one such protocol layer through

12   redirected references to the data packet processing procedures comprised within

13   the at least one such protocol layer;

14   obtaining a logical reference to the processed data packets from the

15   interfaced protocol layer, the logical reference referring to a memory block in the

16   kernel memory space within which the processed data packets are stored; and

17   providing the logical reference to an intrusion detection analyzer

18   executing within user memory space.

1   16.   A storage medium according to Claim 15, further comprising:

2   providing a network hardware interface in a link protocol layer logically

3   located at a device end of the protocol stack;

4   providing an application software interface in a transport protocol layer

5   logically located at a user end of the protocol stack; and

6   tapping the collected data from the protocol stack between and through the

7   link protocol layer and the transport protocol layer.

1   17.   A storage medium according to Claim 15, further comprising:

2   storing incoming data frames in a read queue associated with each

3   protocol layer;

4   storing outgoing data frame in a write queue associated with each protocol

5   layer; and

6   retrieving the logical reference to the processed data packets from at least

7   one of the read queue and the write queue.

1   18.   A storage medium according to Claim 15, further comprising:

2   storing the references to the data packet processing procedures comprised

3   within the at least one such protocol layer in a module switch table in the kernel

4   memory space; and

5   replacing select procedure references in the module switch table with

6   references to data collection procedures in the protocol stack multiplexor.

1   19.   A storage medium according to Claim 18, wherein one such

2   protocol layer comprises a Transmission Control Protocol-compliant (TCP)

3   protocol layer and a further such protocol layer comprises a User Datagram

4   Protocol-compliant (UDP) protocol layer, further comprising:

5   augmenting the procedure references in the module switch table for the

6   procedures for processing data frames for the TCP protocol layer with references

7   to TCP data collection procedures in the protocol stack multiplexor; and

8   replacing the procedure references in the module switch table for the

9   procedures for processing incoming data frames for the UDP protocol layer with

10   references to UDP data collection procedures in the protocol stack multiplexor.

1   20.   A system for detecting network intrusions using a protocol stack

2   multiplexor, comprising:

3   a network protocol stack comprising a plurality of hierarchically

4   structured protocol layers, each such protocol layer comprising a read queue and a

5   write queue for staging transitory data packets and a set of procedures for

6   processing the transitory data packets in accordance with the associated protocol;

7   a protocol stack multiplexor interfaced directly to at least one such

8   protocol layer through a set of redirected pointers to the processing procedures of

9   the interfaced protocol layer, further comprising:

10   a data packet collector referencing at least one of the read queue

11   and the write queue for the associated protocol layer; and

12   a data packet exchanger communicating a memory reference to

13   each transitory data packet from the referenced at least one of the read queue and

14   the write queue for the associated protocol layer; and

15   an analysis module receiving the communicated memory reference and

16   performing intrusion detection based thereon.

1   21.   A system according to Claim 20, further comprising:

2   a module switch table storing a set of pointers to the processing

3   procedures of the interfaced protocol layer; and

4   an initialization module selectively redirecting the set of pointers to a set

5   of data collection procedures comprised in the protocol stack multiplexor.

1   22.   A system according to Claim 21, further comprising:

2   a one-way shim redirecting the set of pointers for processing the transitory

3   data packets for one of the read queue and the write queue for the associated

4   protocol layer.

1   23.   A system according to Claim 21, further comprising:

2   a two-way shim redirecting the set of pointers for processing the transitory

3   data packets for both the read queue and the write queue for the associated

4   protocol layer.

1   24.   A system according to Claim 20, wherein the network protocol

2   stack is a TCP/IP-compliant protocol stack, further comprising:

3   a set of TCP/IP-compliant protocol layers, selected from the group

4   comprising at least:

5   a data link protocol layer;

6   an Internet (IP) protocol layer;

7   an Transmission Control Protocol (TCP) layer; and

8   a User Datagram Protocol (UDP) layer.

1   25.   A method for detecting network intrusions using a protocol stack

2   multiplexor, comprising:

3   executing a network protocol stack comprising a plurality of hierarchically

4   structured protocol layers, each such protocol layer comprising a read queue and a

5   write queue for staging transitory data packets and a set of procedures for

6   processing the transitory data packets in accordance with the associated protocol;

7   interfacing a protocol stack multiplexor directly to at least one such

8   protocol layer through a set of redirected pointers to the processing procedures of

9   the interfaced protocol layer, further comprising:

10   referencing at least one of the read queue and the write queue for

11   the associated protocol layer; and

12   communicating a memory reference to each transitory data packet

13   from the referenced at least one of the read queue and the write queue for the

14   associated protocol layer; and

15   receiving the communicated memory reference into an analysis module

16   and performing intrusion detection based thereon.

1   26.   A method according to Claim 25, further comprising:

2   storing a set of pointers to the processing procedures of the interfaced

3   protocol layer into a module switch table; and

4   selectively redirecting the set of pointers to a set of data collection

5   procedures comprised in the protocol stack multiplexor.

1   27.   A method according to Claim 26, further comprising:

2   redirecting the set of pointers for processing the transitory data packets for

3   one of the read queue and the write queue for the associated protocol layer.

1   28.   A method according to Claim 26, further comprising:

2   redirecting the set of pointers for processing the transitory data packets for

3   both the read queue and the write queue for the associated protocol layer.

1   29.   A method according to Claim 25, wherein the network protocol

2   stack is a TCP/IP-compliant protocol stack, further comprising:

3   defining a set of TCP/IP-compliant protocol layers, selected from the

4   group comprising at least:

5   a data link protocol layer;

6   an Internet (IP) protocol layer;

7   an Transmission Control Protocol (TCP) layer; and

8   a User Datagram Protocol (UDP) layer.